Hindawi
Security and Communication Networks
Volume 2021, Article ID 6673691, 16 pages
https://doi.org/10.1155/2021/6673691

Research Article

A Manipulation Prevention Model for Blockchain-Based E-Voting Systems

Ruhi Taş [1,2] and Ömer Özgür Tanrıöver [1]

[1]*Department of Computer Engineering, Ankara University, Ankara 06830, Turkey*
[2]*Turkish Radio Television Corporation, IT Department, Ankara 06550, Turkey*

Correspondence should be addressed to Ruhi Taş; ruhitas@yahoo.com

Received 20 December 2020; Revised 23 March 2021; Accepted 11 April 2021; Published 28 April 2021

Academic Editor: Vincenzo Conti

Security and trust are seen as the most important issues in electronic voting systems. Therefore, it is necessary to use cryptographic procedures to ensure anonymity, security, privacy, and reliability in these systems. In recent years, blockchain has become one of the most commonly used methods for securing data storage and transmission through decentralized applications. E-voting is one of these application areas. However, data manipulation is still seen as a major potential problem in e-voting systems. In the-proposed model, administrators or miners are prevented from previewing election results which are normally accessible data due to the blockchain structure. A double-layer encryption model is proposed and tested to prevent manipulations that may occur with the election results. It is ensured that the election results can be counted after the participation of all stakeholders at the end. In this way, potential manipulations may be prevented during the election period. As a result of the model, the privacy of voters is ensured, no central authority is needed, and the recorded votes are kept in a distributed structure.

1. Introduction

A fair election is desirable by everyone. Frequently, there are doubts in the minds of voters related to the voting procedures, counting processes, and the announcement of results [1–3]. The election systems have evolved depending on the needs and developments of the time during which they were developed. Technological developments offer possible innovations to every field; likewise, it is thought that digitalization mechanisms to be added to voting systems can minimize human errors [4]. But, unlike paper-based electoral systems, problems such as system failure, network security, and information security may arise with an electronic voting system.

One of the most important issues in e-voting systems is the security weaknesses made by people inside or outside who are authorized to access the system. A decentralized design and cryptographic data storage security approach may have the potential for solving these problems. Normally, cryptography is mainly used to encrypt information such as voter data, votes, and voting results before data are stored on the server. Therefore, the system can ensure the authenticity and security of the voting information [5]. In this context, various additional features and solutions have been proposed to be integrated into election systems. Development work is still ongoing. Different types of improvements to e-voting have been done to provide easy election organization, easy participation, and low cost. Accordingly, various enabling technologies have been adapted ranging from biometric authentication to remote voting [6, 7] to kiosk systems [8] or to mobile voting systems [9]. Nowadays, the security and privacy of blockchain platforms have attracted great attention. Recently, blockchain-based voting systems have been proposed [10–13]. However, it is stated that such systems still have trust problems. Abuidris et al. [14] and Ghosh et al. [15] state the risks and vulnerabilities of blockchain applications. In e-voting systems, the guaranteeing the security of the votes is seen as one of the most important problems. An attacker can copy and decipher passwords if he has sufficient computational power or when

the encryption algorithm is proven unsafe. Therefore, the e-voting system's ability to secure data and defend against potential attacks has always been viewed with suspicion.

On the other hand, due to its privacy features, homomorphic encryption has been used in other studies [16–20]. Operations such as adding and multiplying on the message encrypted with homomorphic encryption can be done using the Paillier algorithm [20]. However, the proposed structures should be carefully examined. Although homomorphic encryption is generally agreed to be secure, for example, in the scheme proposed by Li et al. [12] and analysis conducted by Wang et al. and Qu et al., weaknesses were also identified [21–23]. Fontaine and Galand [24] argue that in general the proposed schemes are not very suitable for every use and their properties should be carefully studied. As e-voting systems contain a vital sequence of processes, the applications should be inspected with care.

In addition, blockchain technology, infrastructures, and its security properties may solve certain security issues identified, and it is emphasized that more studies are needed to adapt and enrich these features to developed desired e-voting systems [25, 26]. It is also known that although the blockchain includes many security measures, for example, attackers can still leak information by analyzing network traffic and transaction information [27].

Alongside these limitations related to the application of blockchain to e-voting, the most important problem in election systems can be seen as the manipulation of election results or the emergence of a situation that may affect the result. In places where the election results go hand in hand, there may be situations that may affect the result with little difference. It is also known that there are such disputes as a result of many elections. One of the most critical issues that can affect the outcome is the risk of results being foreseen by the leading candidate in the constituency. It has been determined that such information can be leaked during the election as a result of storing votes in a central place or being held by malicious people, even in a distributed structure.

Preliminary or forseen results could affect the decisions of other voters. Therefore, it is critical to prevent disclosure of any results during the election period. The main contribution of this work is the following: we proposed a model for e-voting systems that can ultimately combine the security layer of the paper-based system with the security layers of the voting system. As a part of this undertaking, we proposed a model that eliminates data privacy and data reversibility problems that arose during the election.

The general focus wason prevention of data breaches during the election period and proposing requirements for such a suitable decentralized block chain-based electronic voting system. The particular objective of the project was to develop an e-voting system using double-layer encryption that prevents the occurrence of situations that could impact the voter's decision. The system requirements have been defined and performance evaluation was made in the application scenario of the designed system. In the proposed system, the votes are encrypted first, and, secondly, the encrypted votes are divided into pieces and distributed to the nodes. In this way, the data that is open in the blockchain system alone becomes meaningless. To obtain the election results, a certain number of nodes come together to make the data meaningful and then can declare the results. As the results of the proposed model, the privacy of voters was ensured, while it was ensured that there was no central authority, and the recorded votes were kept in a distributed structure. It was guaranteed that the stored data cannot be predicted during the voting, and only the election results could be obtained after the participation of all stakeholders. As a result of the encryption and distribution algorithm together, the time to distribute the data increases according to the number of nodes to be connected.

The rest of this paper is organized as follows. Section 2 provides the literature on e-voting and threats. Section 3 provides a description of the blockchain concepts and the e-voting systems based on blockchain. Section 4 describes the system implemented, encryption methods, and analysis of the implementation. The last section provides the concluding remarks and outlines future work.

2. Literature on E-Voting and Threats

Advances in information technology are also affecting the election processes and methods. Researchers are working to contribute to existing methods and to improve the contribution of such systems to voting systems. Electronic voting is evaluated from different angles to traditional voting systems, such as convenience, reducing the margin of error, and getting quick results.

Election commissions may face various problems during the election. The most common problems are improper approval regarding voting, duplication, or illegal voting. Secure authentication is very important to ensure that the eligible voter actually casts the vote. As an example, regarding the vote duplication problem, Mahiuddin recommended a biometric iris recognition control system integrated into the voting system to avoid duplication [28]. Rana et al. and Olaniyi et al. advised fingerprint scan for the same purpose [29, 30].

Although electronic voting is an interesting topic, some researchers have published studies emphasizing that the shortcomings and risks of these systems need to be investigated comprehensively. Olumide et al. and Kohno et al. also emphasize these risks in their studies [31, 32]. For security reasons, different solutions are recommended as follows: biometric [28,33, 34], fingerprint [29, 30], chip ID card (Near-Field Communication card) [35], and different encryption methods [17, 21, 36, 37], and suggestions are still examined by researchers.

Experts have been working on safe and effective e-voting proposals for more than three decades. In an early article published by Chaum [38] in 1981, an anonymous communication channel to encrypt the ballot is used for the first time. After that, various e-voting systems were used in many countries since the 2000s. Various countries from each continent used e-voting in local and general elections. Some of these are as follows: USA (2000), India (2002), UK (2002), Estonia (2005), Canada (2006), and Norway (2011) [39–42].

E-voting refers to the end-to-end process of registration, voting, and counting on a digital election management platform. Electronic voting systems try to be as easy to use and secure as the ideal traditional choices and eliminate human error. Electronic voting systems can generally be divided into two categories [43]. Ballots can be used remotely, as well as through closed systems allocated in election offices. In pool site electronic voting, the voters still participate physically, but the ballots are discarded and counted electronically. In remote online voting, votes are used remotely, usually using a personal device over the Internet. Such alternative devices can be voting kiosks, computers, mobile devices, paper-based electronic systems, and even televisions [44].

Such applications and systems must be accepted by society. A practical secure e-voting plan should be structured to provide the following features:

Eligibility: only registered and authorized voters can vote [45, 46]

Uniqueness: no one can vote again [46]

Noncoercibility: no one should be able to follow up the person for which candidate he voted for [47]

Reliability: votes must be securely recorded even in case of system malfunctions [48]

Integrity: no one can change the votes [49]

Verifiability: make sure that the votes are counted correctly [9, 50, 51]

Electronic voting mainly is investigated for solving some of the problems identified in traditional voting systems. Earlier purpose of e-voting systems has been to integrate electronic devices into the voting system. However, as a result of this integration, various difficulties are detected. Some research results indicated that serious critical weaknesses were still revealed in current e-voting systems. Various election officials see possibilities for internal or external attackers affecting the illegal election outcome [31]. Hassan and Wang identified a set of possible problems such as unauthorized privilege, seizure, wrong cryptography usage, vulnerabilities to network threats, and software development weaknesses in the systems it examines [50]. Küsters et al. studied several e-voting machines (ThreeBallot, Wombat voting, and Helios voting system) used in actual elections. The study showed that voting machines are vulnerable to attacks being under the assumption of trust in authorities. They showed that the authorities could change the ballot papers in an unnoticeable way and thus manipulate the election without being detected [52].

Halderman and Teague conducted a detailed security analysis of the iVote system used in the elections in New South Wales, Australia, in 2015. As a result of their research, they reported that they detected vulnerabilities that could lead to manipulations or the capture of some private information [53]. In another review, Springall et al. examined in detail the security analysis of the Estonian voting system. They showed how attackers could access election servers or voters' customers to alter election results or undermine the legitimacy of the system [54].

Estonia and USA are two countries that have been using e-voting systems on a large scale. Estonia became the first country in the world to allow online voting in 2007. However, due to the infrastructure problems used in this election system, it was determined that voters could cast more than one vote. It was also revealed that those who had access to the voting system could see partial results beforehand [54, 55]. Elections insiders' attacks such as poll workers and local elections officials are real and imminent threats to electoral integrity [56].

Recently, blockchain technology with distributed architecture features has been proposed for e-voting systems, generally for their benefits in terms of end-to-end verifiability [57]. Like other researchers, Wei and Chang [58] point out that the blockchain can be used in electronic voting systems. Taş and Tanrıöver systematically examined the blockchain voting systems claimed by many schema authors in their study in August 2020. They found that e-voting was still far from being a safe real-life application [42].

A voting systems threat analysis was conducted by the Brennan central task force on the security of electronic voting systems used in the American elections. In this study, mainly the insertion of corrupt software, wireless and other remote control attacks, attacks on tally servers, shutting-off of voting system, they studied different scenarios such as denial-of-service attacks and attacks on the ballot. The results of the study have demonstrated that it may be possible to alter the ballot that the votes shown for one candidate are recorded and counted for another [59].

Another study by Lewis et al. showed that the system developed for Swiss elections had a trap door. The study showed that malicious managers or individuals can manipulate votes. It was stated that even if this breach was closed, it was not known whether other hidden ones were there for such manipulations [60].

In another important scheme called the Prêt à Voter voting scheme [61], security weaknesses have also been detected as a result of tests carried out by independent parties. There is a tradeoff between voting system transparency and the potential for a hacker, an organization, or the government to determine exactly how each voter has voted [62]. The Swiss Post conducted a public test of the e-voting system they developed in 2019. The analysts identified weaknesses [63] that could allow an attacker to change or place votes and produce a result that would not match with the actual voters. These results showed that the system needs to be reverified [60, 64]. Ethical hackers even organize a contest at the DefCon conference about how fast voting machines used in America can be hacked, rather than whether they can be hacked [65].

Although, during the last 5 years, various blockchain-based e-voting systems were proposed, most of the papers only highlight the general and positive characteristics of these systems [42, 66, 67]. As examples, studies in [11, 13, 68] describe their design of a blockchain-based election system. However, most of these studies do not propose a complete design of a voting system. In addition, the weaknesses in blockchain systems recently appeared in some studies

[69, 70]. These challenges are stated as scalability, privacy leak, Man-in-the-Middle attack, and Distributed Denial of Service attack (DDoS) [70]. On the other hand, online voting poses numerous risks to the security of the ballots used as well as to the integrity of the general election system. Moreover, adopting features like blockchain and encryption does not solve many of the underlying security risks inherent in online voting [71]. For this reason, it is important not only to keep the ballots safe but also to prevent them from being used by malicious users.

To summarize, most traditional e-voting systems require a central and reliable third party for their processes. This causes them to be of critical importance in the storage and counting of votes. Blockchain is recommended for its decentralized features and increasing its security features. Despite getting lots of attention, the online voting system is still not widely used. The most important problems in the voting system remain the reliability of the system in storing and counting the votes and the voters' assurance that there will be no manipulation.

3. Blockchain Terms and Concepts

In this section, we give a brief introduction to blockchain related terminology and its basic concepts. The appearance of the blockchain concept appeared in 2009 when "Satoshi Nakamoto" combined blockchain infrastructure with various rules and created the first cryptocurrency, a form of digital money that relied on cryptography for its security [72]. A block can be defined as a data structure that is added as a chain structure in a distributed way [73]. Blockchain can be seen as a distributed ledger of recorded transactions. The validity of transactions is established through a consensus mechanism, and transactions are recorded into blocks in a chain. Decentralization means that there is no central computing device for storing sent transactions [74]. Each blockchain node stores its copy and contains a reference to the previous block hash (Figure 1).

After the rising popularity of Bitcoin, blockchain technology gained popularity in numerous sectors. In a broader sense, the blockchain mechanism consists of a decentralized shared database that provides a secure, immutable, and auditable list of records. It enables anonymous parties to keep and organize their databases altogether in a completely decentralized manner and without the need to establish a centralized administration that implements a common central control [76]. The blockchain provides a permanent record of transactions on a network. Unlike a traditional database, the system copies the chain of records that occur and then allows each participant on the network to view all transactions.

The applications of blockchain range from the Internet of things applications [77] to secure digital rights management [78], pharmaceuticals [79], financial transactions, and trade and commerce [80]. Blockchain development infrastructures are also constantly evolving; however, examples that are widely used are Bitcoin [72], Ethereum [81], Hyperledger, and R3 Corda.

The blockchain infrastructure consists of six layers. From bottom to top, the layer structure is composed of data, network, consensus, incentive, smart contract, and application layer [25, 27, 82, 83] (Table 1).

The function of the data layer is to store the data in the block. A hash function is applied to produce a fixed-length output of variable size data. Being an irreversible one-way function, the processed data cannot be obtained back from the calculated hash value. Thus, a timestamp and a hash function are used for the integrity of the blockchain.

The network layer of the blockchain works on a peer-to-peer (P2P) network structure. Peer-to-peer implementations are generally managed by distributed architectures that divide tasks between peers without a reliable authority [84]. This is used as a network program protocol to communicate, process, and duplicate blockchain between two or more machines. Each node on the network is responsible for its resources, and it serves as both a server and a client.

The consensus layer manages the distributed consensus mechanism that governs the order of blocks. The purpose of the incentive layer is to provide definite incentives to get nodes to participate in the security verification of the blockchain. For contract layer, with the help of smart contract, transactions are initiated according to the rules [27, 83].

3.1. Hash Function. A hash function is an operation that creates a unique value of a fixed length with mathematical functions of various lengths of data. It is a one-way function and the original data cannot be obtained from the summary value obtained. In the hash process, the same value is generated for the same data, but when there is the slightest change, the value created by the hash function also changes.

3.2. Encryption Methods. Ensuring the confidentiality and integrity of data is an important issue. In this paper, the symmetric and asymmetric encryption fundamentals are used to ensure the confidentiality and integrity of data.

Symmetric Encryption. The same key is used in symmetric encryption and decryption steps. AES, DES, 3DES, and RC4 are the main symmetric encryption methods. The encryption key is public, as the decryption key remains private [24]. Symmetric encryption algorithms are much faster and require less computational power, but their main weakness is key sharing. Since the same key is used to encrypt and decrypt information, this key must be shared with anyone who needs access to the data. This naturally creates security risks.

Asymmetric Encryption Schemes. Different keys are used in asymmetric encryption, encryption, and decryption. These keys are referred to as public and private keys. The public key is used for encryption and authentication, while the private key is used for decryption and signing. Asymmetric encryption systems are very slow compared to symmetric systems and require more computational power due to much longer keys.

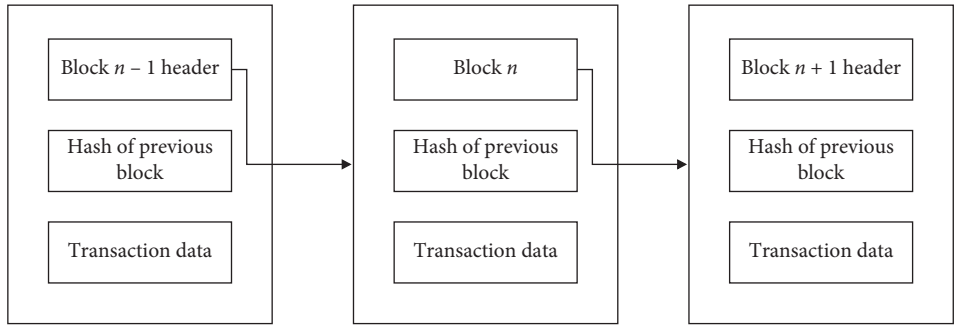

Figure 1: Blockchain data structure [75].

Table 1: Blockchain layer architecture [25, 59, 80].

Layer	Properties
Data	Data + encryption + timestamp
Network	*P2P* network verification
Consensus	Consensus mechanism
Incentive	Smart contract programmed rules

3.3. Digital Signatures. A digital signature is a cryptographic mechanism used to verify the accuracy and integrity of digital data. The process essentially consists of hashing a message along with the signer's private key. The recipient of the message can then check whether the signature is valid using the public key provided by the signer [64].

3.4. Smart Contract. In 1994, the term smart contract was introduced by Nick Szabo, a cryptographer and a computer scientist [85]. According to Szabo's concept, the contracts can be converted into computer code, stored and copied to the system, and controlled by a computer network that runs the blockchain. Smart contracts refer to the writing of a contract in the lines of code and the transactions are executed according to the terms of these contracts which are executed on the blockchain [86]. When the contracts are loaded on nodes, they will interact with other components on the blockchain based on rules. Smart contracts are designed to perform reliable transactions without the need for a central authority or an external application mechanism. The blockchain-based smart contract becomes incrementally popular and has been exploited by multitudinous industries [87].

3.5. Consensus Mechanisms. The establishment of a decision is based on general acceptance by taking a certain number of steps within the framework of certain rules between a group of people. Proof of Work (PoW), Proof of State (PoS), Byzantine Fault Tolerance (BFT), and Delegated Proof of Stake (DPoS) are common consensus mechanisms [88].

Proof of Work (PoW). The most widely used consensus mechanism is Proof of work (PoW). PoW requires a complex problem-solving process. Miners perform complex calculations to reach a hash value with predetermined properties in the PoW protocol. The first miner reaching the specified hash value is entitled to add a new block to the chain. The relevant block is added to the blockchain after the hash value is published to other nodes and the hash value is verified by all nodes. Then, the integrity of the chain is ensured by adding the new block to all miners. At the end of this process, the miner who publishes the block is rewarded [89].

Proof of Stake (PoS). Proof of Stake (PoS) or virtual mining protocol [15] establishes alternative selection tools that aim to keep PoW's benefits while improving on its weaknesses [90]. Proof of Stake (PoS) is an energy-saving compromise protocol alternative to the PoW protocol. The use of PoS started to increase due to the advantage of reducing power consumption and scalability. Miners in the PoS protocol have to prove the ownership of a coin amount (value). In this protocol, people with more assets are more likely to be used for verification [91].

Delegated Proof of Stake (DPoS). Delegated Proof of Stake is similar to PoS, but nodes in the network select delegates for block creation and validation and block validation and validation can be done very quickly with a small number of elected delegates. It makes blocks using DPoS not only faster than PoW or PoS blocks but also less secure. This is because only a small group of people decide the validity of transactions for the entire network and make this mechanism more centralized. Delegates can form cartels or start working together in secret, threatening trust in the entire network [92].

Byzantine Fault Tolerance (BFT). It is the consensus protocol that can still coordinate and come to a consensus despite some difference between the nodes [93].

4. System Description and Analysis

In theory, the decentralization principle of blockchain technology can increase the integrity of elections and their controllability by different entities. The blockchain-based voting design relies on recording each data entry in the ledger across multiple nodes for constant proof of each ballot paper. For our implementation, we have decided to use a private network and use the Ethereum blockchain API. The reason for this decision is that Ethereum is a widely

recognized and proven-secure infrastructure for blockchain applications. On the other hand, as smart contracts are visible and transparent to all voting participants, they are not suitable for storing sensitive data. That is why homomorphic encryption is preferred in our system due to its privacy features. The homomorphism feature allows one to operate on the ciphertexts without decrypting them. For a voting system, this property allows the encrypted ballots to be counted by any third party without leaking any information on the ballot [85, 94].

To protect the sensitive voting data, it was aimed to fragment the data and keep it distributed. Secret data sharing is a technique to strongly distribute fragments of important information between distributed networks. For this reason, the Shamir Secret Share method is applied as the second layer of security [95].

The proposed system scheme and proposed algorithm can be viewed in Figure 2 and Algorithm 1. The system procedures that should be conducted at every stage are briefly as follows:

Phase 1: ID Card Delivery. Fingerprint/biometric data loaded microchip ID card distribution (Figure 3).

Phase 2: Preregistration. Central Authority provides a list that is based on only eligible voters who can vote. Generally, the list of voters is held by election administrators. The election manager updates the list of eligible voters before the election if needed (Figure 3).

Phase 3: Registration.Voters apply for voting services with an ID card containing fingerprint/biometric data. These data can be checked with the help of an independent special device. The voting service office manager checks the person's right to vote. If he/she is authorized, he/she is provided to select an account in a closed envelope (Figure 3).

Phase 4: Voting: The voter selects candidates. The voter votes in any of the electronic cabinets with the help of the account information given in the envelope to him/her.

Phase 5: Transaction: At this stage, the vote is first encrypted with homomorphic encryption (Figure 4). It is then divided into pieces (Figure 5). Then, the transfer of transactions to all nodes is included in the system.

Phase 6: Counting: Authority and assigned nodes to complete the process of combining the data for counting. Other nodes verify the results. It should achieve the same results.

The operations performed in the flowchart of the proposed system are shown in Figure 2. In the first phase, every citizen should be provided with (Ci) biometric ID card. All the necessary information is uploaded to these chip cards.

Election management authority is responsible for the election system requirements. System administrators and election authorities are to organize and control the voting process by initializing the system parameters and triggering different phases of an election.

Election authority prepares voter list (Vi ← Ci), and the system administrator defines the election (Eid)), candidate list (CLi), and registration office (RegOfficeID).

Registration office authority guarantees the authorization for each voter (Vi). After the authentication is verified, the voter gets a token. This token can only be used once. After the candidate (CLi) selection, encrypted vote transaction begins (Figures 4 and 5). Voters can submit their votes from multiple points applying the following:

$$\text{Encrypted Chipher Ballot} \leftarrow \text{Secret Share Slicer}\ (\text{Homomorphic Enc}\,(\text{CLi})). \tag{1}$$

This ballot is being distributed to the whole blockchain nodes in the voting phase. If the following transaction data is valid, it is added to the blockchain (Figure 6).

$$\text{Send Ballot Transaction}\ (\text{Token, ChipherBallot, Eid, Registration OfficeID, time stamp, Pub key}). \tag{2}$$

We can summarize the vote encryption phase (Figures 4 and 5); the important parameters of the applied methods are formally as follows (plaintext refers to vote information).

Let p and q be random prime numbers, and then calculate

$$n = p.q,$$
$$\lambda(n) = \text{lcm}\,(p-1, q-1), \tag{3}$$
$$(\text{lcm} : \text{lowest common multiple}).$$

If random prime numbers p and q have the same lengths, generator $g = n + 1$ can be chosen. If not, then choose random$g \in Z^*_{n^2}$,

$$n \text{ and } g\,(\text{public}),\ p \text{ and } q\,(\text{private}), \tag{4}$$

where x expresses the decimal value of the selected candidate and y indicates the encrypted value corresponding to this value.

$$x\,(\text{plain text}),\ y\,(\text{chiper text}), \tag{5}$$

where r value is chosen to provide randomness.

$$r\,(\text{random number})0 < r < n,\ r \in Z^*_n. \tag{6}$$

Encryption: $y = \text{Enc}\,(x, r) = g^x \cdot r^n \bmod n^2$.

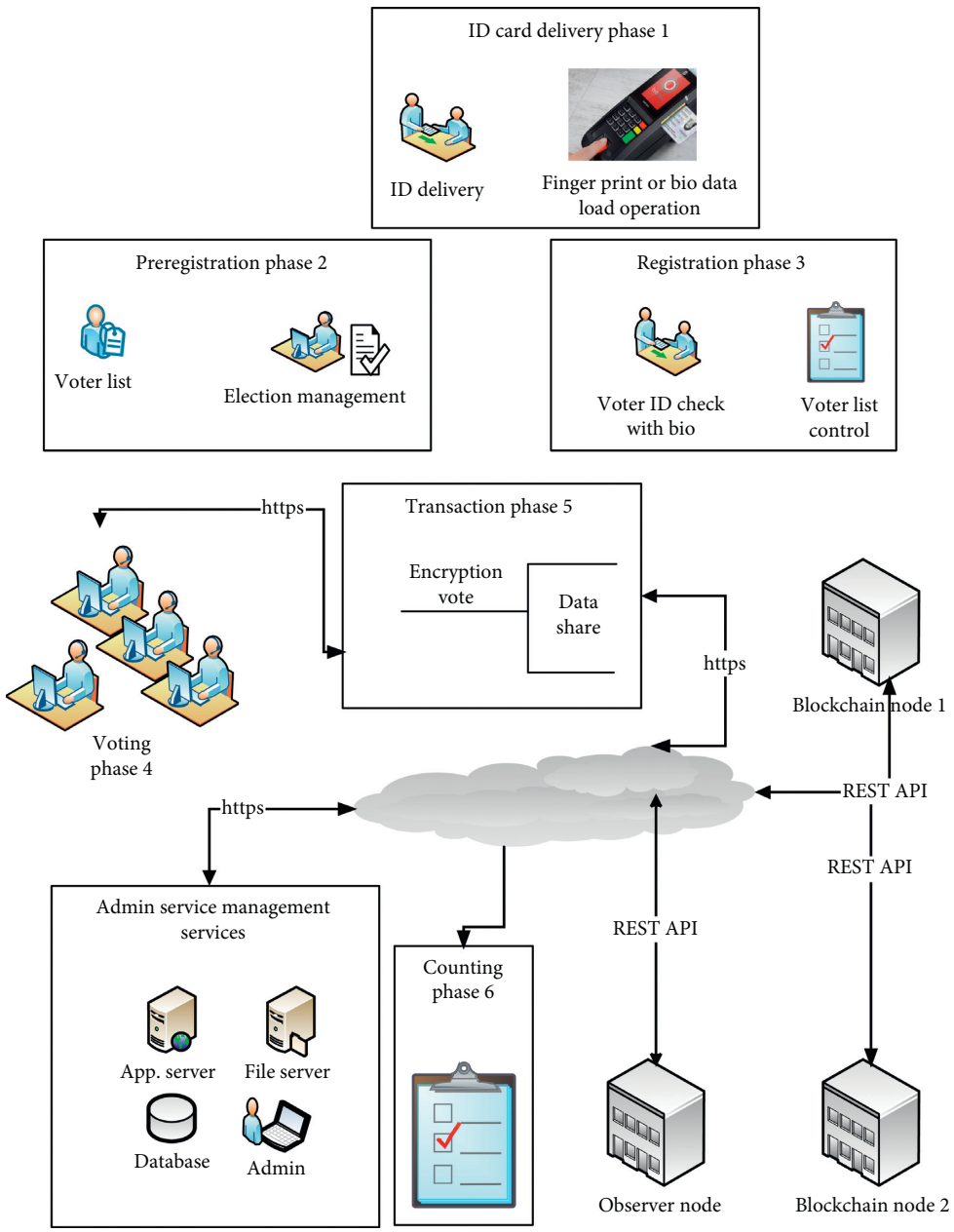

Figure 2: Proposed blockchain voting model extended from [42].

Table 2 illustrates sample random encryption calculation.

$$\text{All Votes} := \prod \text{Enc}(x, r) \bmod n^2,$$

$$x = \text{Dec}(y) = \frac{L\left(y^{\lambda} \bmod n^2\right)}{L\left(g^{\lambda} \bmod n^2\right)} \bmod n, \tag{7}$$

$$L(u) = \frac{(u-1)}{n},$$

$$L\left(y^{\lambda} \bmod n^2\right) = L1,$$

$$L\left(g^{\lambda} \bmod n^2\right) = L1$$

Decryption:

$x = \text{Dec}(y) = L(y^{\lambda} \bmod n^2)/L(g^{\lambda} \bmod n^2) \bmod n = L1/L2.$

The table of encryption durations (Table 3) for each user was examined in practice tests, and it was found that computation ended within an average of 93 ms.

After the conversion of the decrypted value to binary, we can find the counting result for each candidate.

$$\text{Convert to Binary } (x) = (\text{Count A})\ (\text{Count B})\ (\text{Count C}). \tag{8}$$

The anonymity and confidentiality of the votes used are ensured by homomorphic encryption. However, although the votes cast are encrypted and stored, there is a possibility that they can be counted at the nodes that store the data in

Input: Voter ID
Output: Sliced Encrypted Ballot
(1) **Begin**
(2) **If** Voter Id in Voter List Id **then**//Check Voter
(3) Get the voter Token, set the password
(4) **else** not an eligible voter exit
(5) **if** (voter Id in registered voter list) **then**//check registered Voter
(6) Check Token and Password
(7) **else** not registered voter exit
(8) **if** not voted (token and password) **then**
(9) chose Candidate ID
(10) chipherData = HomomorphicEnc(Candidate ID)//data encryption
(11) chiperBallot = SecretShareSlicer (chipherData) //data share
(12) send chiperBallot to blockchain nodes
(13) **else** failed login exit
(14) **END**

Algorithm 1: Voting algorithm.

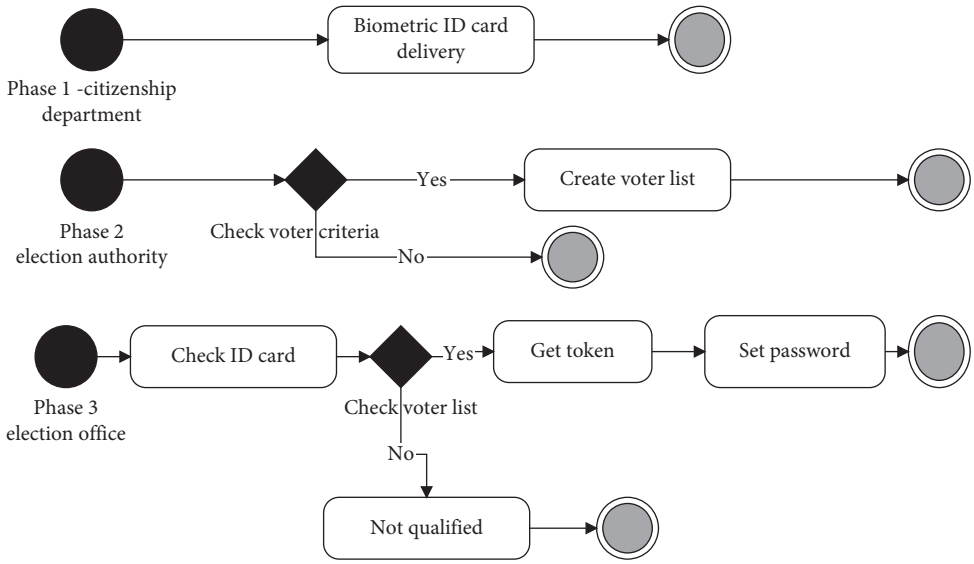

Figure 3: Flowchart of ID card delivery and registration phase.

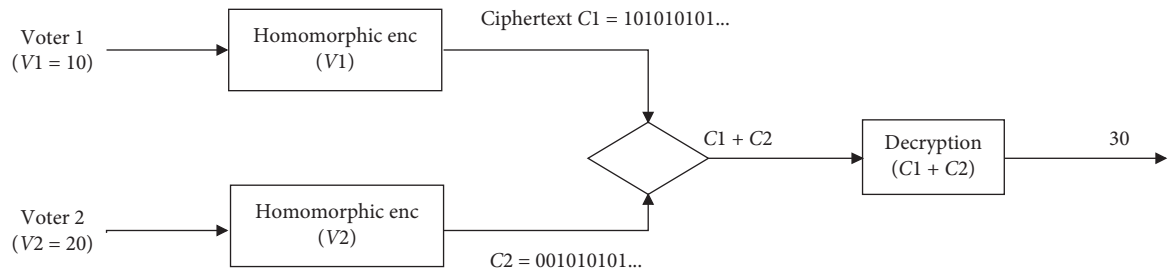

Figure 4: Encrypt ballot, homomorphic addition.

the blockchain. For this reason, it is thought that the problem can be solved if this encrypted data can be distributed among the nodes and, after the election, a certain number of nodes can come together to form the original data. Private sharing is achieved thorough dividing the private information into smaller chunks or shares and then distributing those shares across the group or network. Instead of sending encrypted votes directly to the nodes, the data will be fragmented and sent to the nodes and stored. It is aimed to be reconstructed by gathering a certain number of

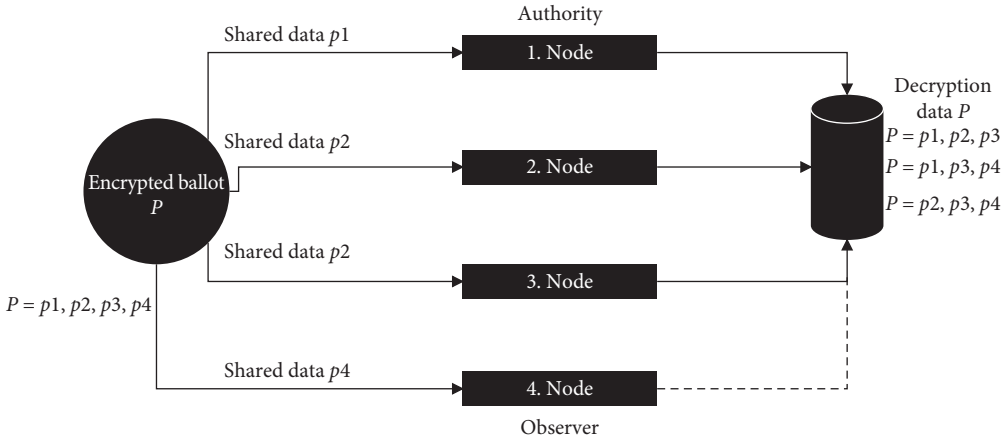

Figure 5: Encrypted data share diagram.

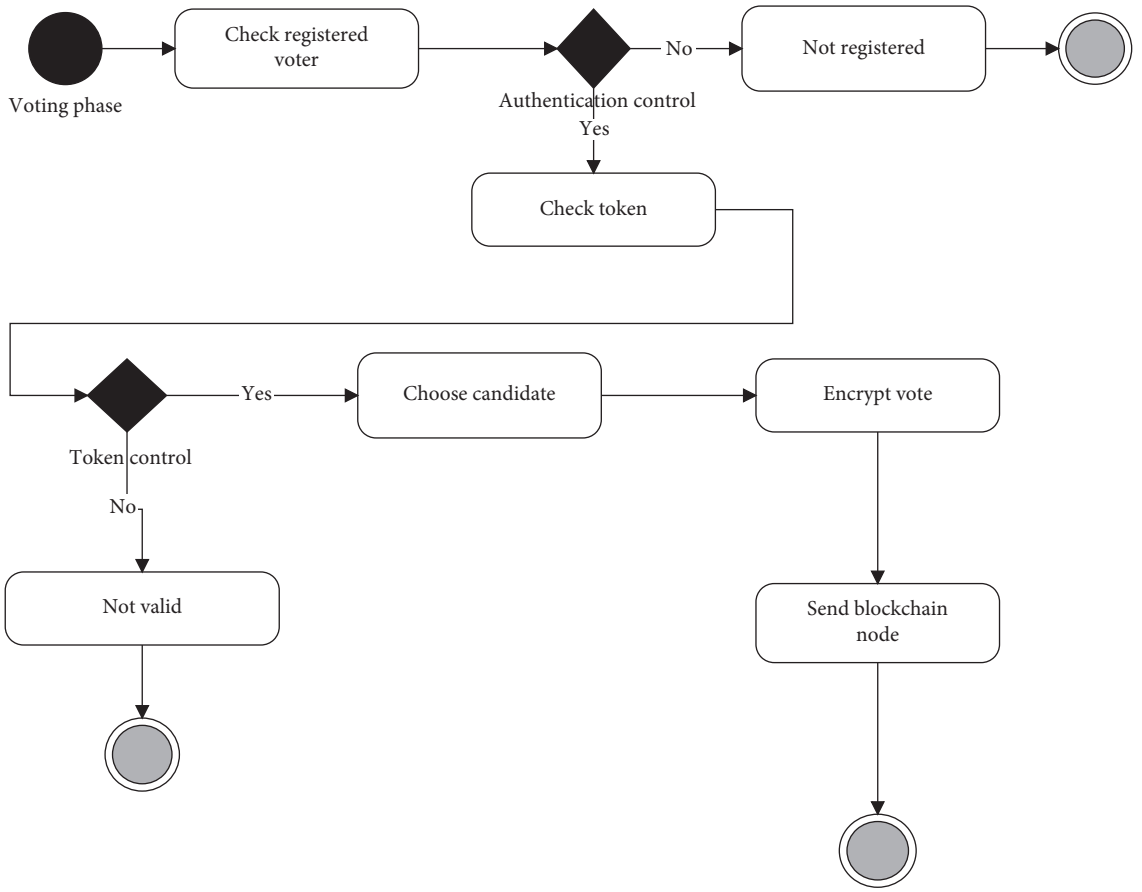

Figure 6: Flowchart of the voting phase.

Table 2: Vote and random encryption calculation.

Vote	A 2^4	B 2^2	C 2^0	x	Random number r	Enc $(x,r) = g^x r^n \bmod n^2$ $g = n+1$, n^2
1	x			16	131	Enc (16,131)
2		x		4	161	Enc (4,161)
3			x	1	83	Enc (1,83)
4	x			16	160	Enc (16,160)
5		x		4	62	Enc (4,62)
6	x			16	81	Enc (16,81)
7			x	1	135	Enc (1,135)

Table 3: Encryption durations.

Voters	Encryption duration (ms)
1	94
2	89
3	91
4	87
5	90
6	93
7	107

nodes during the count. The structure created in this way will ensure that both redundancy and data integrity are met with certain criteria.

As shown in Algorithm 2,

vote data is fragmented into 4 nodes, P ($p1$,$p2$,$p3$,$p4$) (Figure 5);

the number of nodes decided in the design comes together to ensure data integrity, P = decryption ($p1$,$p2$,$p4$);

the same numbers of different nodes come together and verify. P = decryption ($p2$,$p3$,$p4$).

$$\begin{aligned}
&\mathrm{P} = \text{random prime number, } a_1 \text{ an } d\, a_2 \text{ random number,}\\
&\mathrm{S} = \text{secret data,}\\
&\mathrm{p} \in \mathbb{P}\colon\ \mathrm{p} > S,\ p > n,\\
&\mathrm{a_i} < p,\ \mathrm{a_o} = \mathrm{S},\\
&f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1},\\
&a_0 = S
\end{aligned} \tag{9}$$

$N = 5$ and $k = 3$ (5 nodes, at least 3-node threshold).

$$f(x) = a_0 + a_1 x + a_2 x^2. \tag{10}$$

For 5 nodes, data are spitted into 5 pieces. This data fragmentation process is distributed according to the entire number of nodes and provides cross-checking by combining random nodes to create and control them.

$$\begin{aligned}
D_0 &= (1, f(1) \bmod p) = (1, y_0),\\
D_1 &= (2, f(2) \bmod p) = (2, y_1),\\
D_2 &= (3, f(3) \bmod p) = (3, y_2),\\
D_3 &= (4, f(4) \bmod p) = (4, y_4),\\
D_4 &= (5, f(5) \bmod p) = (5, y_5),
\end{aligned} \tag{11}$$

Original data is obtained with at least 3 nodes randomly selected for recovery (Figure 7).

$$\begin{aligned}
&(x_0, y_0) = (1, y_0),\\
&(x_1, y_1) = (2, y_1),\\
&(x_2, y_2) = (4, y_2).
\end{aligned} \tag{12}$$

$$\begin{aligned}
&f(x) = \textstyle\sum_{j=0}^{2} y_j \cdot l_j(x),\\
&l_j(x) \coloneqq \prod_{0 \le m \le k} \frac{x - x_m}{x_j - x_m} = \frac{x - x_0}{x_j - x_0} \cdots \frac{x - x_k}{x_j - x_k}, m \ne j,\\
&\qquad\qquad k = 3\,(0, 1, 2) \quad j = 0 \quad m \ne 0,\\
&l_0(x) = \frac{(x - x_1)}{(x_0 - x_1)} \frac{(x - x_2)}{(x_0 - x_2)},\\
&\qquad\qquad k = 3\,(0, 1, 2) \quad j = 1 \quad m \ne 1,\\
&l_1(x) = \frac{(x - x_0)}{(x_1 - x_0)} \frac{(x - x_2)}{(x_1 - x)_2},\\
&\qquad\qquad k = 3\,(0, 1, 2) \quad j = 2 \quad m \ne 2,\\
&l_2(x) = \frac{(x - x_0)}{(x_2 - x_0)} \frac{(x - x_1)}{(x_2 - x_1)},\\
&f(x) = \textstyle\sum_{j=0}^{2} y_j \cdot l_j(x).
\end{aligned} \tag{13}$$

Fragmented values from each node are used to recover the function.

$$f(x) = y_0 \cdot l_0(x) + y_1 \cdot l_1(x) + y_2 \cdot l_2(x). \tag{14}$$

Finally, hidden data is obtained by calculating the p mod of the function.

$$f(x) = a_2 x^2 + a_1 x + a_0 \,(\bmod p). \tag{15}$$

Secret data $S = a_0$ can be obtained from Algorithm 3.

Nodes or observers can check the validity of all transactions, making sure the election as a whole is secure and the data is stored consistently. The data-sharing scheme prevents even an attacker with unlimited computing power from accessing data alone. To obtain the data, it must have enough shares to meet the minimum number of shares.

For secret share, the computation times with fixed thresholds (Figure 8) and with fixed nodes (Figure 9) were calculated. Threshold refers to the minimum number of nodes that need to come together when the value stored in fragmented nodes is to be recovered. It was determined that the increase in the number of nodes when the threshold remains constant causes an increase in the computation time, but the change is linear. However, when the number of nodes was fixed and when the threshold value was increased, it was determined that there were significant increases in the calculation time.

This showed that using optimum nodes and thresholds in real system design will significantly reduce the voting processing time. In our experiments, 600 nodes and 300

N nodes, P random prime
Input: Secret data $a_0 = S$
Output: Shared data $(x_i, y_j)i = 0, \ldots, N-1$
(1) $(a_i)_{i=1,\ldots,N-1} \leftarrow$ Rand //calculation function coefficients
(2) **for** $i = 0$ **to** N **do**//calculate function
(3) $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{N-1} x^{N-1}$
(4) **for** $j = 0$ **to** N **do**//calculate slices
(5) $y_j \longleftarrow f(j) \bmod P$
(6) **return** $(x_i, y_j)i = 0 \ldots N-1$

Algorithm 2: Secret sharing algorithm.

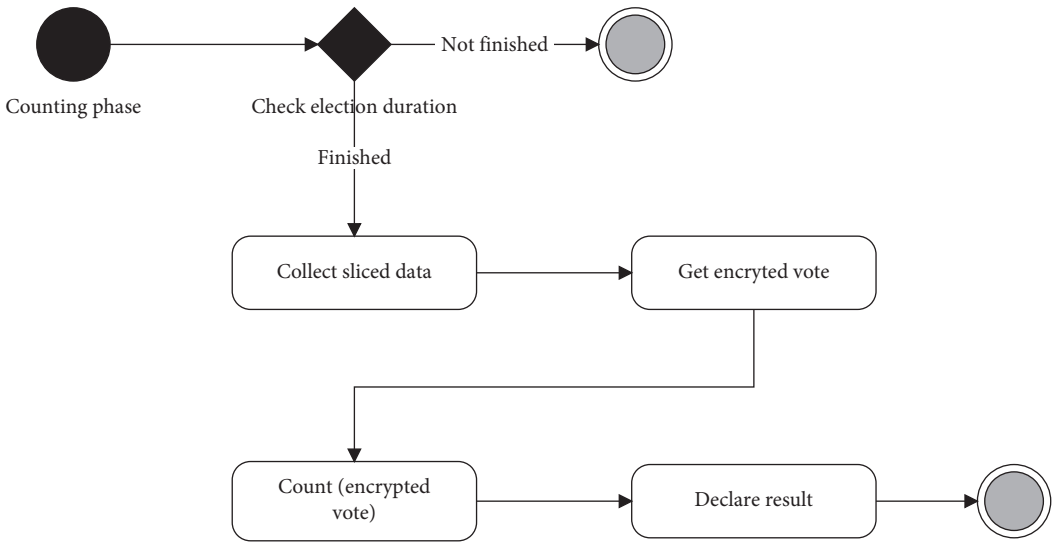

Figure 7: Flowchart of vote counting phase.

N nodes, P prime number
Input: $(x_i - y_j)i = 0..N\text{-}1$
Output: Secret data S
(1) **for** $j = 0$ **to** k **do**//calculation of function coefficients from nodes
(2) $l_j(x) = (x - x_0)/(x_j - x_0)(x - x_k)/(x_j - x_k), k \neq j$
(3) **for** $j = 0$ **to** N **do**//reconstruct function
(4) $f \longleftarrow = y_0 \cdot l_0(x) + y_1 \cdot l_1(x) + y_{j-1} \cdot l_{j-1}(x).$
(5) $S \longleftarrow f \bmod P$//calculate encrypted data
(6) **return** S

Algorithm 3: Secret reconstruction algorithm.

thresholds are considered in the acceptable range. Considering redundancy, security, and efficiency, the experimented values were acceptable, taking into account these three criteria. It was observed that when the threshold value was increased, the voting time increased logarithmically, and this negatively affected the election time. In addition, when a lower value is selected, the possibility of causing manipulation again arises. At this setting, it took about 7000 ms. ~ 1.17 sec. (encryption + share + transaction = 93 + 1171 + 5774) for the ballot to deliver to the blockchain network. However, this duration is expected to be higher real-life elections when more simultaneous nodes with high loads are needed; where for example more than 150 million Americans voted in the last USA presidential election held on November 3, 2020 [96].

The dependability problem that may arise in e-voting will be reduced by using a printout vote and putting it in a bullet box as in classical voting. In this way, a hybrid structure may be established with ballots stored for final control. In our case, the security of the voting system is ensured by combining the use of a fingerprint ID card in the voting protocol, the use of homomorphic encryption, and the distributed structure of data. This method can be integrated into any private blockchain system. The occurrence

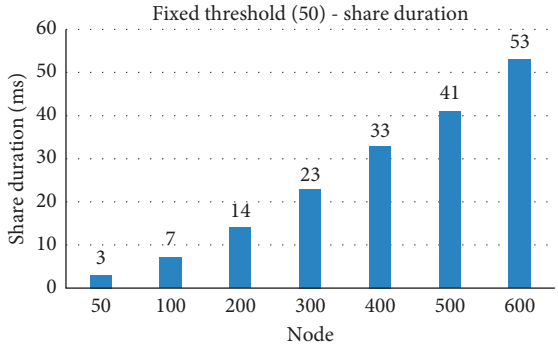

Figure 8: Fixed threshold (50) share duration.

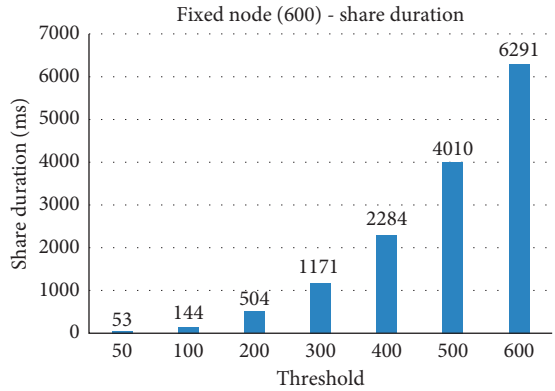

Figure 9: Fixed node (600) share duration.

of information leaks related to ballot information andelection results and use of multiple votes can be prevented .

An analysis of properties can be stated as follows:

Privacy: All voters are allowed to vote with a randomly generated account, while no password or username to connect with people is used. All votes cast start a transaction with homomorphic encryption first. In this way, the privacy of the voter is protected.

Availability: Being in a distributed permission structure, the availability percentage of the system increases. Its closed structure provides resistance to attacks.

Eligibility: since voters accepted by biometric data control are allowed to vote, only those who are authorized to vote are enabled to vote.

Uniqueness: Once registered for voting, the voter cannot vote again and can only vote once with his account. A smart contract does not normally allow such operations.

Noncoercibility: Random key based encryption and distribution prevent tracking of votes with the combination of homomorphic encryption and secret share modeling. The user account to be used to vote is randomly created and is not tied to people and the vote cast.

Reliability: Keeping the votes cast in a distributed structure enables the system to work in any situation. No data is lost. The distributed nature of the system ensures higher durability against attacks when compared to single-point systems.

Integrity: Data stored on the blockchain is safe from tampering. Since the proposed system has a permission based blockchain structure and a framework with different nodes, the data in this system is secure.

Verifiability: Firstly, in reaching the final results, the process is the aggregation of information of a certain number of nodes included in the consortium. Secondly, other nodes work on a consensus mechanism and hence cross-check and verify the results. Since the printed votes will be cast in the box in the election room, the net result can be calculated with the box count in case of need.

Buying attack: It is recommended to use the voting process similar to the classical voting process by means of legal sanctions. In this way, people are not allowed to show whom they voted for.

Replay attack, Sybil attack or Man-in-the-Middle attack: Although the system uses permission based private network, there may be Man-in-the-Middle attacks, replay attacks, or Sybil attacks. In case of incidents related to imitation of voters or attempts to change the vote cast, the results may be verified by cross counting the votes in the election offices.

5. Conclusion

Although electronic voting has been a topic of interest for many years, it is still not fully resolved. Online voting systems contain a security conflict such that it may be possible for authorities to conduct fraud or do manipulations which are difficult to detect by other participants.

In this work, a double-layer security model is proposed and tested to prevent manipulations that may occur during the elections and with the election results. It is ensured that the election results can be counted after the participation of all stakeholders. As a result of the model, the privacy of voters is ensured, no central authority is needed, and the recorded votes are kept in a distributed structure. In this way, potential manipulations may be prevented during the elections.

Validation through simulation results showed that the voting and counting phases of the proposed system worked as intended. Ballots are encrypted with homomorphic encryption and then shared among nodes in the system. Only valid voter ballots are guaranteed to be recorded as transactions, which were mined into blocks. It was also tested that the system continues to work even if a node becomes inoperable. Furthermore, it is ensured that the election results are announced with all stakeholders without data loss.

The most important limitation has been the difficulty of simulations with as many nodes as a real election system needs. In the future, it is aimed to simulate with a more realistic system, to operate the system from end to end, and to focus on optimizations for scalability of the system. Another future work is that in the proposed system the end

of election is assumed to be depending on the system time. However, the system may be improved to increase the security of the time dimension.

In our opinion, transition to the e-voting method should proceed slowly by implementing in small pilot populations first and then widening the scope slowly. The implementation of such voting systems still poses many challenges and risks for developers and governments.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] S. Shukla, A. N. Thasmiya, D. O. Shashank, and H. R. Mamatha, "Online voting application using ethereum blockchain," in *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, pp. 873–880, Bangalore, India, September 2018.

[2] M. Achieng and E. Ruhode, "The adoption and challenges of electronic voting technologies within the South African context," *International Journal of Managing Information Technology*, vol. 5, no. 4, pp. 1–12, 2013.

[3] S. Nichter, "Vote buying or turnout buying? Machine politics and the secret ballot," *American Political Science Review*, vol. 102, no. 1, pp. 19–31, 2008.

[4] J. Blanc, "Challenging the norms and standards of election administration," *Electronic Voting*, vol. 31, 2007.

[5] S. S. Shinde, S. Shukla, and D. K. Chitre, "Secure E-voting using homomorphic technology," *International Journal of Emerging Technology and Advanced Engineering*, vol. 3, no. 8, pp. 203–206, 2013.

[6] S. Komatineni and G. Lingala, "Secured E-voting system using two-factor biometric authentication," in *Proceedings of the 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC)*, pp. 245–248, Iccmc, Erode, India, March 2020.

[7] D. Gentles and S. Sankaranarayanan, "Application of biometrics in mobile voting," *International Journal of Computer Network and Information Security*, vol. 4, no. 7, pp. 57–68, 2012.

[8] M. G. Gurubasavanna, S. Ulla Shariff, R. Mamatha, and N. Sathisha, "Multimode authentication based electronic voting kiosk using raspberry pi," in *Proceedings of the International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), I-SMAC*, pp. 528–535, Palladam, India., September 2018.

[9] A. Khelifi, Y. Grisi, D. Soufi, D. Mohanad, P. V. S. Shastry, and " M-Vote, "M-Vote: a reliable and highly secure mobile voting system," in *2013 Palestinian International Conference on Information and Communication Technology*, pp. 90–98, Gaza, Israel, April 2013.

[10] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling blockchain: a data processing view of blockchain systems," *IEEE Transactions on Knowledge and Data Engineering*, vol. 30, no. 7, pp. 1366–1385, 2018.

[11] G. C. Prasetyadi, A. Benny, and R. Refianti, "Blockchain-based electronic voting system with special ballot and block structures that complies with Indonesian principle of voting," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 1, pp. 164–170, 2020.

[12] K. Curran, "E-voting on the blockchain," *The Journal of British Blockchain Association*, vol. 1, no. 22–7, 2018.

[13] M. Audi Ghaffari, *An E-Voting System Based on Blockchain and Ring Signature*, School of Computer Science University of Birmingham, Birmingham, UK, 2017.

[14] Y. Abuidris, A. Hassan, A. Hadabi, and I. Elfadul, "Risks and opportunities of blockchain based on e-voting systems," in *Proceedings of the 2019 16th International Computer Conference on Wavelet Active Media Technology and Information Processing*, pp. 365–368, Chengdu, China, December 2019.

[15] A. Ghosh, S. Gupta, A. Dua, and N. Kumar, "Security of Cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects," *Journal of Network and Computer Applications*, vol. 163, Article ID 102635, 2020.

[16] S. Bai, G. Yang, J. Shi, G. Liu, and Z. Min, "Privacy-Preserving oriented floating-point number fully homomorphic encryption scheme," *Security and Communication Networks*, vol. 2018, Article ID 2363928, 14 pages, 2018.

[17] L. Li, R. Lu, K.-K. R. Choo, A. Datta, and J. Shao, "Privacy-Preserving-outsourced association rule mining on vertically partitioned databases," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 8, pp. 1847–1861, 2016.

[18] M. S. Rahman, I. Khalil, A. Alabdulatif, and X. Yi, "Privacy preserving service selection using fully homomorphic encryption scheme on untrusted cloud service platform," *Knowledge-Based Systems*, vol. 180, pp. 104–115, 2019.

[19] A. Huszti, "A homomorphic encryption-based secure electronic voting scheme," *Publicationes Mathematicae Debrecen*, vol. 18, 2011.

[20] S. M. Anggriane, S. M. Nasution, and F. Azmi, "Advanced e-voting system using Paillier homomorphic encryption algorithm," in *Proceedings of the 2016 International Conference on Informatics and Computing (ICIC)*, pp. 338–342, Mataram, Indonesia, October 2016.

[21] B. Wang, Y. Zhan, and Z. Zhang, "Cryptanalysis of a symmetric fully homomorphic encryption scheme," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 6, pp. 1460–1467, 2018.

[22] Q. Qu, B. Wang, Y. Ping, Z. Zhang, and M. Zhang, "Improved cryptanalysis of a fully homomorphic symmetric encryption scheme," *Security and Communication Networks*, vol. 2019, pp. 1–6, Article ID 8319508, 2019.

[23] R. Frankland, D. Demirel, J. Budurushi, and M. Volkamer, "Side-channels and eVoting machine security: identifying vulnerabilities and defining requirements," in *Proceedings of the 2011 International Workshop on Requirements Engineering for Electronic Voting Systems*, pp. 37–46, Trento, Italy, August 2011.

[24] C. Fontaine and F. Galand, "A survey of homomorphic encryption for nonspecialists," *EURASIP Journal on Information Security*, vol. 2007, pp. 1–10, 2007.

[25] B. K. Mohanta, D. Jena, S. S. Panda, and S. Sobhanayak, "Blockchain technology: a survey on applications and security privacy Challenges," *Internet of Things*, vol. 8, p. 100107, 2019.

[26] B. Samban, Y. Ramesh, M. S. Rao, T. C. Rao, and N. P. Patnaik M, "Blockchain approach to cyber security vulnerabilities attacks and potential countermeasures," *International Journal of Security and Its Applications*, vol. 14, no. 1, pp. 1–14, 2020.

[27] H. Wang, Y. Wang, Z. Cao, Z. Li, and G. Xiong, "An overview of blockchain security analysis," in *in Cyber Security*, X. Yun, W. Wen, B. Lang et al., Eds., Springer, Berlin, Germany, 2019.

[28] M. Mahiuddin, "Design a secure voting system using smart card and Iris recognition," in *Proceedings of the 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE)*, pp. 1–6, Cox's Bazar, Bangladesh, February 2019.

[29] M. F. Rana, A. Altaf, and S. Z. Naseem, "Enhanced real time system of evoting using finger print," in *Proceedings of the 2013 International Conference on Electronics, Computer and Computation (ICECCO)*, pp. 297–300, Ankara, Turkey, November 2013.

[30] O. M. Olaniyi, T. A. Folorunso, A. Ahmed, and O. Joseph, "Design of secure electronic voting system using fingerprint biometrics and CryptoWatermarking approach," *International Journal of Information Engineering and Electronic Business*, vol. 8, no. 5, pp. 9–17, 2016.

[31] A. Olumide, B. Olutayo, and S. E. Adekunle, "A review of electronic voting systems: strategy for a novel," *International Journal of Information Engineering and Electronic Business*, vol. 12, no. 1, pp. 19–29, 2020.

[32] T. Kohno, A. Stubblefield, A. D. Rubin, and D. S. Wallach, "Analysis of an electronic voting system," in *Proceedings of the IEEE Symposium On Security And Privacy, 2004*, pp. 27–40, Berkeley, CA, USA, March 2004.

[33] T. Illakiya, S. Karthikeyan, U. M. Velayutham, and N. T. R. Devan, "E-voting system using biometric testament and cloud storage," in *Proceedings of the 2017 Third International Conference On Science Technology Engineering & Management (ICONSTEM)*, pp. 336–341, Chennai, India, March 2017.

[34] A. Jamkar, O. Kulkarni, A. Salunke, and A. Pljonkin, "Biometric voting machine based on fingerprint scanner and arduino," in *Proceedings of the 2019 2nd International Conference on Intelligent Communication and Computational Techniques (ICCT)*, pp. 322–326, Jaipur, India, September 2019.

[35] S. M. Hasan, A. M. Anis, H. Rahman, J. S. Alam, S. I. Nabil, and M. K. Rhaman, "Development of electronic voting machine with the inclusion of Near Field Communication ID cards and biometric fingerprint identifier," in *Proceedings of the 2014 17th International Conference on Computer and Information Technology (ICCIT)*, pp. 383–387, Dhaka, Bangladesh, December 2014.

[36] S. Bartolucci, P. Bernat, and D. Joseph, "Sharvot," in *Proceedings of the 1st International Workshop On Emerging Trends In Software Engineering For Blockchain - WETSEB '18*, pp. 30–34, Gothenburg, Sweden, March 2018.

[37] S. Panja and B. K. Roy, "A secure end-to-end verifiable e-voting system using zero knowledge based blockchain," *International Association for Cryptologic Research*, vol. 54, 2018, https://eprint.iacr.org/2018/466.pdf.

[38] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp. 84–90, 1981.

[39] D. Clarke and T. Martens, ""E-voting in Estonia," 2020, http://arxiv.org/abs/1606.08654.

[40] R.. B. Venkatapur, B. Prabhu, A. Navya, R. Roopini, and S. A. Niranjan, "Electronic voting machine based on blockchain technology and aadhar verification," *International Journal of Innovations in Engineering and Science*, vol. 3, pp. 12–15, 2018.

[41] N. Goodman and J. Pammett, "The patchwork of internet voting in Canada," in *Proceedings of the 2014 6th International Conference on Electronic Voting: Verifying the Vote (EVOTE)*, pp. 1–6, Bregenz, Austria, October 2014.

[42] R. Taş and Ö. Ö. Tanrıöver, "A systematic review of challenges and opportunities of blockchain for E-voting," *Symmetry*, vol. 12, no. 8, p. 1328, 2020.

[43] J. P. Gibson, R. Krimmer, V. Teague, and J. Pomares, "A review of E-voting: the past, present and future," *Annals of Telecommunications*, vol. 71, no. 7-8, pp. 279–286, 2016.

[44] Á. Cserny and A. Nemeslaki, "The challenges of e-voting," *Public Policy and Administration*, vol. 17, no. 4, pp. 497–509, 2018.

[45] W. Zhang, Y. Yuan, Y. Hu et al., "A privacy-preserving voting protocol on blockchain," in *Proceedings of the 2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, pp. 401–408, San Francisco, CA, USA, July 2018.

[46] F. S. Hardwick, A. Gioulis, R. N. Akram, and K. Markantonakis, "E-voting with blockchain: an E-voting protocol with decentralisation and voter privacy,," in *Proceedings of the IEEE 2018 International Congress on Cybermatics: 2018 IEEE Conferences on Internet of Things*, pp. 1561–1567, Halifax, Canda, August 2018.

[47] T. Dimitriou, "Efficient, coercion-free and universally verifiable blockchain-based voting," *Computer Networks*, vol. 174, Article ID 107234, 2020.

[48] P. Y. A. Ryan, S. Schneider, and V. Teague, "End-to-End verifiability in voting systems, from theory to practice," *IEEE Security & Privacy*, vol. 13, no. 3, pp. 59–62, 2015.

[49] L. C. Bollinger and M. A. McRobbie, "Ensuring the integrity of elections," in *Securing The Vote: Protecting American Democracy*, pp. 103–105, National Academies of Sciences, Bengaluru, Karnataka, 2018.

[50] A. Hassan and X. Zhang, "Design and build a secure e-voting infrastructure," in *Proceedings of the 2013 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, pp. 1–7, Farmingdale, NY, USA, May 2013.

[51] G. S. Grewal, M. D. Ryan, L. Chen, and M. R. Clarkson, "Du-vote: remote electronic voting with untrusted computers," in *Proceedings of the IEEE 28th Computer Security Foundations Symposium*, pp. 155–169, Verona, Italy, July 2015.

[52] R. Kusters, T. Truderung, and A. Vogt, "Clash attacks on the verifiability of E-voting systems," in *Proceedings of the 2012 IEEE Symposium on Security and Privacy*, pp. 395–409, San Francisco, CA, USA, May 2012.

[53] J. A. Halderman and V. Teague, "The new south wales ivote system: security failures and verification flaws in a live online election," 2020, http://arxiv.org/abs/1504.05646.

[54] D. Springall, T. Finkenauer, Z. Durumeric et al., "Security analysis of the Estonian internet voting system," in *Proceedings of the 2014 ACM SIGSAC Conference On Computer And Communications Security*, pp. 703–715, Scottsdale, AZ, USA, March 2014.

[55] J. Bannet, D. W. Price, A. Rudys, J. Singer, and D. Walach, "Hack-a-vote: security issues with electronic voting systems," *IEEE Security & Privacy Magazine*, vol. 2, no. 1, pp. 32–37, 2004.

[56] A. Yasinsac, "Insider threats to voting systems," in *Proceedings of the 2010 Workshop on Governance of Technology, Information and Policies - GTIP '10*, pp. 1–8, Austin, TX, USA, September 2010.

[57] N. Shanthi, R. Suvitha, and R. C. Suganthe, "Blockchain based e-voting approach IN P2P network," *Journal of Critical Reviews*, vol. 7, no. 9, 2020.

[58] C. C. Zheng Wei and C. C. Wen, "Blockchain-based electronic voting protocol," *JOIV : International Journal on Informatics Visualization*, vol. 2, no. 42, p. 336, 2018.

[59] L. Norden, "The machinery of democracy: protecting elections in an electronic world," 2006, https://www.brennancenter.org/sites/default/files/publications/Machinery%20of%20Democracy.pdf.

[60] S. J. Lewis, O. Pereira, and V. Teague, "The use of trapdoor commitments in bayer-groth proofs and the implications for the verifiabilty of the scytl-swisspost internet voting system," 2019, https://people.eng.unimelb.edu.au/vjteague/UniversalVerifiabilitySwissPost.pdf.

[61] P. Y. A. Ryan, D. Bismark, J. Heather, and S. Schneider, "À voter: a voter-verifiable voting system," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 4, pp. 662–673, 2009.

[62] M. Eldridge, "A trustworthy electronic voting system for australian federal elections," 2018, http://arxiv.org/abs/1805.02202.

[63] R. Kuenzi, "These are the arguments that sank e-voting in switzerland," 2020, https://www.swissinfo.ch/eng/e-voting_these-are-the-arguments-that-sank-e-voting-in-switzerl;/45136608.

[64] P. Grontas and A. Pagourtzis, "Blockchain, consensus, and cryptography in electronic voting," *Homo Virtualis*, vol. 2, no. 1, p. 79, 2019.

[65] Y. Hermstrüwer, "The limits of blockchain democracy: a transatlantic perspective on blockchain voting systems," *Stanford-Vienna Transatlantic Technology Law Forum*, vol. 32, 2020, https://law.stanford.edu/wp-content/uploads/2020/01/hermstruewer_wp49.pdf.

[66] N. Kshetri and J. Voas, "Blockchain-enabled E-voting," *IEEE Software*, vol. 35, no. 4, pp. 95–99, 2018.

[67] S. Pawar, R. Pawar, P. Dhomse, and J. Suryavanshi, "Evoting. using blockchain," *Telematics and Informatics*, vol. 5, no. 12, pp. 455–458, 2018.

[68] C. K. Adiputra, R. Hjort, and H. Sato, "A proposal of blockchain-based electronic voting system," in *Proceedings of the 2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, pp. 22–27, London, UK, October 2018.

[69] J. J. Xu, "Are blockchains immune to all malicious attacks?" *Financial Innovation*, vol. 2, no. 1, p. 25, 2016.

[70] R. Stephen and A. Alex, "A review on BlockChain security," *IOP Conference Series: Materials Science and Engineering*, vol. 396, Article ID 012030, 2018.

[71] S. Greenhalgh, S. Goodman, P. Rosenzweig, and J. Epstein, "Email and internet voting: the overlooked threat to election security," 2018.

[72] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," 2008, https://bitcoin.org/bitcoin.pdf%20.

[73] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: current status, classification and open issues," *Telematics and Informatics*, vol. 36, pp. 55–81, 2019.

[74] J. Lyu, Z. L. Jiang, X. Wang, Z. Nong, M. H. Au, and J. Fang, "A secure decentralized trustless E-voting system based on smart contract," in *2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 570–577, Rotorua, New Zealand, August 2019.

[75] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: architecture, consensus, and future trends," in *Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress)*, pp. 557–564, Honolulu, HI, USA, June 2017.

[76] K. Lauslahti, J. Mattila, and T. Seppala, "Smart contracts how will blockchain technology affect contractual practices?" *SSRN Electronic Journal*, vol. 68, 2018.

[77] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: the case study of a smart home," in *Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pp. 618–623, Kona, HI, USA, March 2017.

[78] Z. Ma, M. Jiang, H. Gao, and Z. Wang, "Blockchain for digital rights management," *Future Generation Computer Systems*, vol. 89, pp. 746–764, 2018.

[79] L. Ismail, H. Materwala, and S. Zeadally, "Lightweight blockchain for healthcare," *IEEE Access*, vol. 7, pp. 149935–149951, 2019.

[80] B. Chen, Z. Tan, and W. Fang, "Blockchain-based implementation for financial product management," in *Proceedings of the 2018 28th International Telecommunication Networks and Applications Conference (ITNAC)*, pp. 1–3, Sydney, Australia, November 2018.

[81] D. Khoury, E. F. Kfoury, A. Kassem, and H. Harb, "Decentralized voting platform based on Ethereum blockchain," in *Proceedings of the 2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET)*, pp. 1–6, Beirut, Lebanon, November 2018.

[82] X. Yan, Q. Wu, and Y. Sun, "A homomorphic encryption and privacy protection method based on blockchain and edge computing," *Wireless Communications and Mobile Computing*, vol. 2020, no. 1, pp. 1–9, Article ID 8832341, 2020.

[83] M. S. Ferdous, M. J. M. Chowdhury, M. A. Hoque, and A. Colman, "Blockchain Consensus Algorithms: A Survey," 2001, http://arxiv.org/abs/2001.07091.

[84] Y. He, H. Li, X. Cheng, Y. Liu, C. Yang, and L. Sun, "A blockchain based truthful incentive mechanism for distributed P2P applications," *IEEE Access*, vol. 6, pp. 27324–27335, 2018.

[85] B. Yu, "Platform-independent secure blockchain-based voting system," *International Association for Cryptologic Research*, vol. 45, 2018, https://eprint.iacr.org/2018/657.pdf.

[86] K. Sadia, M. Masuduzzaman, R. K. Paul, and A. Islam, "Blockchain based secured e-voting by using the assistance of smart contract," 2019, http://arxiv.org/abs/1910.13635.

[87] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Generation Computer Systems*, vol. 107, pp. 841–853, 2020.

[88] A. Kaur, A. Nayyar, and P. Singh, "Blockchain," in *Cryptocurrencies And Blockchain Technology Applications*, G. Shrivastava, D. Le, and K. Sharma, Eds., pp. 25–42, Wiley, Hoboken, NJ, USA, 1st edition, 2020.

[89] M. Saad, L. Njilla, C. Kamhoua, J. Kim, D. Nyang, and A. Mohaisen, "Mempool optimization for defending against DDoS attacks in PoW-based blockchain systems," in *Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pp. 285–292, Seoul, South Korea, May 2019.

[90] S. Leonardos, "Weighted voting on the blockchain : improving consensus in proof of stake protocols," 2018.

[91] S. Leonardos, D. Reijsbergen, and G. Piliouras, "Weighted voting on the blockchain: improving consensus in proof of Stake protocols," in *Proceedings of the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pp. 376–384, Seoul, South Korea, May 2019.

[92] Y. Luo, Y. Chen, Q. Chen, and Q. Liang, "A new election algorithm for DPos consensus mechanism in blockchain," in *Proceedings of the 2018 7th International Conference on Digital Home (ICDH)*, pp. 116–120, Guilin, China, November 2018.

[93] V. Gramoli, "From blockchain consensus back to Byzantine consensus," *Future Generation Computer Systems*, vol. 107, pp. 760–769, 2020.
[94] K. Balasubramanian and M. Jayanthi, "A homomorphic crypto system for electronic election schemes," *Circuits and Systems*, vol. 07, no. 10, pp. 3193–3203, 2016.
[95] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, 1979.
[96] US election results 2020: joe Biden defeats Donald Trump to win presidency, 2020, https://www.theguardian.com/us-news/ng-interactive/2020/dec/08/us-election-results-2020-joe-biden-defeats-donald-trump-to-win-presidency.